

Protecting Critical Information Networks

As society becomes more reliant on digital information systems, cyberterrorism looms as an increasing threat to national and international security, in private as well as government sectors. While evolving technologies improve information systems and critical networks, internet security must rush to match the sophistication and determination of those who seek to compromise these systems.

A collaborative effort seeks to protect and improve the survivability of critical information networks. The Complex Problems Group (CPG) is working to develop methods to detect network intrusions and to support a highly available information network for mission-critical computer systems. The research has been supported by the U.S. Department of Defense.

Complex Problems Group

CPG is the research division of the University of South Carolina Advanced Solutions Group, an information technology development team. CPG includes faculty advisors and researchers from many disciplines who use advanced methods to address problems that cannot be solved by traditional approaches. The group uses theoretical physics, mathematics, and computer science, often with complex computer models, to study problems within the physical, biological, and social sciences.

One of the strengths of CPG is its unique perspective afforded by its diverse membership. Prominent associates include theoretical and nuclear physicists, mathematicians, computer programmers, and other experts from several universities. The Department of Defense has recognized the importance of the group's research by awarding it one of only nineteen fellowships among twelve universities nationwide. The postdoctoral Fellow supports CPG and adds research expertise in wavelet-based applications.

To improve the survivability of critical information networks, project research and development includes two important parts. The first part has established a highly available network for mission-critical computer systems across the United States. The second part has involved advanced research to discover new methods to monitor networks and to detect intrusions.

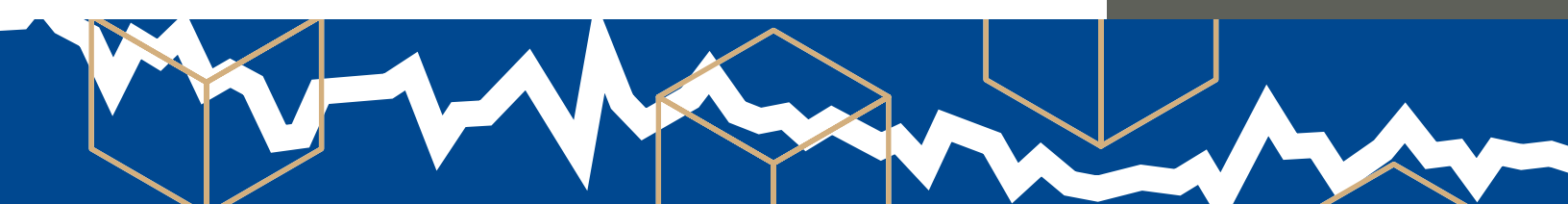
High Availability Information Network

To engineer a high availability information network, the project has first established three robust servers in the Eastern, Western, and Pacific regions of the United States. The computers use a complex network hierarchy to improve functional reliability of a robust emergency information system. The goal of the high availability network is to prevent denial of service caused by the incapacitation of any one site.



Critical Applications for the Real World

- Protect Critical Data
- Establish Reliable Networks
- Detect Network Intrusion in Real Time
- Improve Security and Survivability



An Interest in Complex Problems

- Chaos Theory
- Markov Processes
- Fibonacci Sequences
- Random Matrix Theory
- Particle and Nuclear Physics
- Uncertain Logic and Numbers



Jones Physical Sciences Center
712 Main Street, Ste. 402
Columbia, SC 29208

tel: 803.576.5573
fax: 803.777.3065

CPG website: cpg.psc.sc.edu
ASG website: www.uscasg.org

The project seeks to achieve high reliability in the network by randomly exchanging a primary system server with replicate servers. The important features of the network are the differences in hardware locations and operating environments and the flexibility of configuration. The network uses multiple Internet and Intranet paths to link the servers from high performance computing centers at the University of South Carolina, the University of Utah, and Maui, Hawaii.

The project uses the network to replicate a robust database that contains operations management and critical incident information for emergency preparedness in South Carolina. The replicated database contains critical information needed during preparation and response to disaster incidents. The system tracks incidents, resource requests, critical facilities, bioterrorism response, donated goods, and other information vital to prevention and response of disaster incidents.

Monitoring Networks to Detect Intrusions

The second part of the project has developed a new approach to monitor networks and to detect hostile intrusions. Methods used in physics to study complex systems are applied to analyze network information flow. Findings offer a basis to build software that detects intrusions in the earliest stages of a possible attack. This software would allow rapid detection of network intrusions and help protect networks.

Employing theoretical physics and mathematical methods to analyze network behavior, researchers have discovered a unique method to describe information flow. By identifying characteristics to distinguish normal traffic from hostile network intrusions, the project introduces analysis, reporting, and predictive techniques to identify real-time threats to local and wide area networks.

The research sets a framework to develop new software that will detect a network intrusion during the reconnaissance stage, before it becomes a full attack. Such new software can greatly improve network security and critical network survivability.

Applications to the Real World

The CPG Defense project, through both parts, contributes great benefits to improve survivability of critical information networks. The high availability information network protects critical data by using replication to establish a reliable network. The project thus improves survivability of a critical emergency information system through a wide area network across the United States.

The advanced physics research in the second part offers to support software development to detect real-time network intrusion in the reconnaissance stage. Such development can greatly impact the security of local and wide area networks for commercial as well as government information networks.